VIDEO SURVEILLANCE INFORMATION

Art. 13 Reg. UE 2016/679 "GDPR"

DATA CONTROLLER

VISAF S.R.L.
VIA RINALDONI, 16
60030 SERRA DE' CONTI (AN)
INFO@VISAF.COM

WHAT IS THE PURPOSE OF THE TREATMENT?

In compliance with the regulatory provisions provided for the processing of personal data, we inform you, as a "Data Subject", on the methods of use of personal data concerning you that may be acquired by means of the video surveillance system active at our Company, so as to ensure a correct, lawful and transparent processing in respect of you in compliance with the principles of application placed to protect your personal rights and freedoms.

SU ON WHAT LEGAL BASIS DO WE PROCESS DATA?

We process your data for the protection of the safety of individuals who for any reason are present in the company premises and for the prevention to acts of vandalism, damage misappropriation of movable or immovable property present in the company premises. The processing is carried out, in accordance with the provisions of the GDPR and the April 8, 2010 Measure of the Supervisory Authority for the Protection of Personal Data and the Guidelines 3/2019 on the processing of personal data through video devices, in particular in accordance with Article 6 GDPR Paragraph 1(f), for the legitimate interests of the owner and users, such as the protection of property and personal safety.

WHAT CATEGORIES OF DATA DO WE PROCESS?

Primarily, we only request and process personal data categorized as "common," such as your images/videos while passing through the video surveillance areas. Only in certain cases may the images/videos capture "special" data, but these are assumptions compatible with the stated purposes and legal bases. Videosurveilled areas will be identifiable by signs indicating the "minimum" information with a clearly visible format and placed before the range of the cameras.
The acquisition of your data is necessary for the pursuit of the purposes of processing.

TO WHOM DO WE DISCLOSE PERSONAL DATA?

Your personal data will not be disclosed to other parties and will never be disseminated.
If appropriate, it may be entrusted to companies that carry out activities on behalf of the Owner appointed as External Managers and instructed to process the data in accordance with the regulations in force or transmitted, upon express request, to the Police.

HOW DO WE PROCESS DATA?

We process your personal data at the company premises, in digital format. We take all useful technical and organizational measures to avoid problems of unauthorized access, disclosure, modification or destruction.
Only personnel expressly authorized by the Data Controller, may have access to perform the operations of viewing the footage. Access to the recorded images may only be carried out in the event that any wrongdoing and/or significant events are detected or reported, or when a request to that effect is received from the Judicial Authority.
The Data Controller will ensure that the processing is carried out without determining an unjustified interference in the fundamental rights and freedoms of the data subjects with respect to the purposes of the processing; in particular, it will comply with the prohibition set forth in Article 4 of Law 300/1970 regarding the remote control of employees' work activities. Recording, except in specific cases, is set in h24 mode. No automatic decision-making systems, including profiling, are used.

IS DATA TRANSFERRED TO COUNTRIES OUTSIDE THE EU?

Your data will not be transferred to third countries outside the European Union and with data protection regulations that are not aligned with the EU Regulation 2016/679; moreover, it will not be subject by us to any dissemination to unauthorized third parties for purposes other than those stated in this policy.

HOW LONG DO WE STORE THE DATA?

Your personal data will be stored for a time not exceeding 7 days after collection, considering the specific security needs pursued, related to the purposes of safeguarding the company's assets as well as protecting the safety of people and allowing the control and reconstruction of everything that happens, in case of a request by the Police. The retention of personal data for a period of seven days is deemed necessary for the protection of company assets also in view of the incidents of attempted thefts and other sensitive circumstances that have occurred in the area around the company. The system is programmed to operate full automatic deletion of information after the aforementioned period expires so that the deleted data cannot be reused.

WHAT ARE YOUR RIGHTS?

You can request directly to the Data Controller to see, correct, delete or restrict the data we process that concerns you. He also has the right to data portability, meaning that in certain situations he can request a digital copy of the data or automatic transfer between public entities.

He/she has the right to be informed about the identification details of the Data Controller and Data Processor as well as the purposes, legal basis and other information provided under Articles 13-14 of the GDPR.

He/she has the right to obtain, at the care of the Data Controller, without delay and in any case no later than 30 days from the date of receipt of the request, or 45 days, after notice to the data subject in case of justified reason, access to his/her data, with due clarification:

i. The practical application of Article 15(4) of the GDPR may adversely affect the rights of other data subjects. Indeed, a video recording may contain the personal data of other data subjects. A request by a data subject to want to receive a copy of a recording, pursuant to this article, could adversely affect the rights and freedoms of those data subjects. To avoid this side effect, the Owner may not disclose the video to prevent other subjects from being identified.

ii. A request for access may be unresponsive if, pursuant to Article 11(2) GDPR, the Data Controller is unable to identify the data subject. To this end, the data subject must specify in his or her request the reference period (e.g., a time limit or location). If the Data Controller is unable to comply with the request or the request is not possible, it must notify the data subject.

iii. Pursuant to Article 12 of the GDPR, in the case of excessive or manifestly unfounded requests by the data subject, the Data Controller may alternatively charge a reasonable fee pursuant to Article 12(5)(a), not exceeding the actual costs incurred and including personnel costs, or refuse to process the request (Article 12(5)(b)). The excessiveness of the request must be substantiated and demonstrated.

Any application will be evaluated and possibly granted within the terms of the law, having regard to the limits provided for in Articles 2 undecies and 2 duodecies of the Privacy Code, as amended following the entry into force of Legislative Decree 101/2018, and Article 23 of the GDPR.

In the event of a negative outcome to the application, the interested party has the right to file a complaint before the Guarantor Authority for the Protection of Personal Data, without prejudice to the possibilities of administrative and jurisdictional protection provided by the current legislation.

If you have any doubts, if we keep incorrect or incomplete data, or if you think we have mishandled your personal data, please send a request to the Data Controller, using the "Request Form Exercise of the Rights of the Data Subject," which can be downloaded from the institutional website and can be found at the offices, or by registered letter or by pec.